IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	**3:18-CR-00097**
	:	
v.	**:**	**(Judge Mariani)**
	:	
ROSS ROGGIO	**:**	**(Electronically Filed)**

DEFENDANT'S BRIEF IN SUPPORT OF HIS MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF THE UNITED STATES CONSTITUTION

Procedural History

On March 20, 2018, Ross Roggio was charged in an indictment with conspiracy to commit an offense against the United States, in violation of 18 U.S.C. § 371; violations of the Arms Export Control Act, 22 U.S.C. § 2778(b) and (c); and the International Emergency Powers Act, 50 U.S.C. §§ 1702 and 1705(c); smuggling goods from the United States, in violation of 18 U.S.C. §§ 554 and 2; wire fraud, in violation of 18 U.S.C. § 1343; and money laundering, in violation of 18 U.S.C. §§ 1956(a)(2)(A) and 2. (Doc. 1). On March 23, 2018, Mr. Roggio appeared before Magistrate Judge Karoline Mehalchick for an initial appearance and arraignment, and entered a plea of "not guilty" to the charges.

The instant case is unusual and complex and involves an indictment that includes 37 Counts as well as a Criminal Forfeiture. For this reason, and because

of the extensive amount of discovery initially disclosed, which includes some 10,000 emails and several thousand pages of bank records and other data, Mr. Roggio filed a Motion to Designate Complex Case on September 21, 2018. (Doc. 37). That motion was granted by Order dated October 12, 2018. (Doc. 39).

The matter was originally assigned to Assistant Federal Public Defender Melinda C. Ghilardi who retired from the Federal Defender's Office on February 28, 2019. Prior to her retirement, the case was reassigned to undersigned counsel. As a result of the change in counsel, and the highly complicated nature of the matter, the pretrial motions deadline was continued a number of times and is currently set for March 29, 2019.

Factual Background

The Allegations Against Mr. Roggio

The allegations against Mr. Roggio are contained in the 26-page indictment which contains 37 separate counts against him. In short, Mr. Roggio is accused of unlawfully exporting defense services and defense articles to Iraq and Iraqi foreign nationals. (Doc. 1, pp. 8-9). The Indictment alleges that Mr. Roggio, together with two unindicted co-conspirators, purchased firearm parts in the United States and exported them to Iraq without having first obtained the requisite approval from the Department of State. (*Id*.). According to the Indictment, the purpose of the conspiracy was to construct and operate a factory in Iraq that manufactured and

assembled fully automatic rifles. (Doc. 1, p. 9). Mr. Roggio is alleged to have, at least in part, constructed and operated a firearms manufacturing plant in Iraq and to have supplied that plant with parts that were manufactured in the United States and improperly shipped to Iraq. (Doc. 1, pp. 10-11). These allegations are based on an interpretation of reports, budgets, spreadsheets, emails, *et cetera,* that were obtained by the Government through a forensic search of Mr. Roggio's electronic devices (that search being the topic of this motion). (*See*, Indictment, Doc. 1, pp. 10-11).

In addition to the numerus offenses charged relating to the alleged smuggling of arms parts out of the United States and into Iraq, and the construction of an arms factory in Iraq, Mr. Roggio is charged with numerous fraud offenses and money laundering. (Doc. 1, pp. 17-22). Again, those counts are based, in large part, on an interpretation of reports and emails that were obtained through what Mr. Roggio maintains was an improper and unconstitutional forensic search of his electronic devices, including his personal computers.

The Search and Seizure of Mr. Roggio's Electronic Devices

On March 21, 2017, a Special Agent with the Department of Homeland Security applied for a search and seizure warrant for an Apple MacBook Pro laptop computer, an iPad Tablet Computer, a removable flash drive and smart phones (hereinafter collectively referred to as "electronic devices") owned by Ross Roggio

that had already been seized by the Government on February 26, 2017, and had already been forensically searched. (Exhibit A). The seizure of Mr. Roggio's electronic devices took place at the John F. Kennedy International Airport (JFK) when Mr. Roggio returned to the United States from Turkey on February 26, 2017. The initial seizure and extensive forensic search of the electronic devices was purportedly conducted as a "border search." (Exhibit A, ¶4, footnote 1). However, as discussed below, and as will be more fully developed at a hearing on this motion, the seizure of Mr. Roggio's electronic devices and their subsequent forensic search cannot be considered to have constituted a "border search" under the circumstances in this case. Moreover, to the extent that any part of the interaction at the JFK airport could be considered to be a border search, the seizure of Mr. Roggio's electronic devices, and subsequent unauthorized forensic search, exceeded the permissible scope of such a search and was not justified.

According to the search warrant application, the investigation of Ross Roggio began on March 30, 2016, when the FBI was contacted by a parts manufacturer, Drill Masters Eldorado Tool, Inc, regarding a "suspicious" shipment of gun parts to Iraq. (Exhibit A, ¶17). The application states that a Drill Masters representative told the FBI that it was contacted by an employee of a shipping company called The Package Place, who advised it that gun parts manufactured by Drill Masters were being shipped by Ross Roggio's wife in Pennsylvania to Ross

Roggio in Iraq. (*Id*.). The application further states that "[i]n April of 2016, the DOP was contacted by the FBI and notified that an investigation was ongoing into the activities of Roggio" regarding the export of controlled items to Iraq. (*Id*. at ¶18). Ross Roggio was telephonically interviewed by the FBI on April 29, 2016. (*Id*. at ¶19). The FBI then contacted Drill Masters again on May 2, 2016, and the Package Place employee on May 3, 2016, regarding the above mentioned shipment. (*Id*. at ¶¶ 21-23). On May 16, 2016, Drill Masters forwarded paperwork to the FBI regarding purchases purportedly made by Ross Roggio. (*Id*. at ¶18). The Government then sought, and received, a warrant to obtain certain Yahoo email accounts purportedly used by Ross Roggio. The warrant was executed on November 17, 2016, and emails dating from 2013 through 2016 were received by the Government. (*Id*. at ¶ 31). The affidavit references of two these e-mails. (*Id*. at ¶¶ 34-35). The first contained a document purportedly entitled "Weapons and Ammunition Feasibility Report" which referenced the requisite approval of the Department of State in order to manufacture guns outside of the United States. The second e-mail referenced details of the purchase of various gun parts, but had no indication as to where they were shipped. (*Id*).

The above summarizes the information provided in the March 21, 2017, application for a search and seizure warrant of Mr. Roggio's electronic devices (which were seized almost a month prior and already subject to a forensic search)

that referenced information and events before the February 26, 2017, "border search." The application to seize and search the electronic devices, then provided exacting details of the forensic search that had already occurred. The affidavit states that on February 25, 2017, an investigator in the Roggio matter received notice that Ross Roggio would be arriving at JFK the following day. A secondary border search was then arranged prior to Mr. Roggio's arrival. (Exhibit A, ¶42). Accordingly, the "border search" was a mere pretext to seize Mr. Roggio's electronic devices given that Mr. Roggio had already been under investigation for the preceding 11 months. The application then indicates that Mr. Roggio's electronic devices were seized upon his arrival at JFK and then shipped from the JFK airport to a Homeland Security forensics lab in Philadelphia. The forensics examination revealed, *inter alia*, 8,462 emails from 2001 through 2017, (Exhibit A, ¶58), text, chat, instant messages, call logs, web history and image location information for 2013 through 2017, (Exhibit A, ¶92). The affidavit then provides an over 20-page detailed description of the information forensically obtained to support seizing the devices already in the Government's possession and searching those very electronic devices which had already been searched. (*See* Exhibit A, ¶¶58-118). This information, forensically obtained prior to the issuance of a warrant, was used to obtain the Indictment issued against Mr. Roggio.

Argument

This motion challenges the manner in which Mr. Roggio's electronic devices were seized and forensically searched. While the Government did indeed ultimately apply for and receive a warrant to search the electronic devices, the reasons justifying the issuance of a warrant were obtained during a search those very electronic devices that occurred *prior* to the application for the warrant. Moreover, it appears that the allegations that were made against Mr. Roggio in the Indictment were not based on information obtained as a result of the warrant, but rather on the information that was forensically obtained prior to the application for a warrant was even filed. The Government seeks to justify this intrusion based on the border search doctrine. However, the pretext of a border search cannot justify the seizure and subsequent forensic search of Mr. Roggio's electronic devices. Moreover, the seizure that occurred at the JFK airport, and the forensic search that ensued in the following weeks cannot be considered a proper border search.

The Border Search Doctrine

As this Honorable Court recently recognized, the "border search exception 'is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained.'" *United States v. Lora*, No. 3:16-CR-91, 2019 WL 346410, at *4 (M.D. Pa. Jan. 28, 2019) (*quoting United States v. Ramsey*, 431 U.S. 606, 621 (1977)). "International airports can be considered the

'border' for purposes of border searches." *Id.* (quotation omitted). While routine searches at the border, not based on probable cause and conducted without a warrant, are permissible to protect the integrity of the nation's borders, the type of intrusion presented in this matter, and under the unique circumstances presented herein, present a different situation, outside the scope of the border search exception.

The Third Circuit outlined the permissible bounds of a border search in *United States v. Whitted*, 541 F.3d 480 (3d Cir. 2008) as follows:

> Provided that a border search is routine, it may be conducted, not just without a warrant, but without probable cause, reasonable suspicion, or any suspicion of wrongdoing... This is because the expectation of privacy is less at the border than in the interior and the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is ... struck much more favorably to the Government. Even at the border, however, an individual is entitled to be free from unreasonable search and seizure and his or her privacy interests must be balanced against the sovereign's interests. Consequently, certain searches, classified as "nonroutine," require reasonable suspicion of wrongdoing to pass constitutional muster. Border searches thus fall into two categories: routine searches that require no suspicion and nonroutine searches that require reasonable suspicion.

Id. at 485. Under this framework, it must be first determined whether the search and seizure of Mr. Roggio's electronic devices was indeed a proper border search and, if so, whether it was initially justified and whether the search and continued

seizure of his devices improperly exceeded the permissible scope of a border search. In applying for a search and seizure warrant for the very devices that it had already seized and forensically searched, the Government itself recognized that fourth amendment boundaries existed here, this Honorable Court is called upon to determine whether those boundaries were violated.

This Was Not a Border Search

We know from the affidavit in support of the search warrant that investigators were interested in Ross Roggio some eleven months prior to his arrival at JFK on February 26, 2017. Investigators looked into his purchases from a parts manufacturer, inquired into a package that was purportedly sent to him in Iraq (the contents of which were unknown); the FBI even called him and obtained and read his emails. Yet based on all of that, there was absolutely no indication that Mr. Roggio had done, or was doing, anything wrong. But the Government was interested in looking at Mr. Roggio. What occurred at the JFK airport on February 26, 2017, was not a border search but rather an end run around the warrant requirement in an effort to further the investigation of Mr. Roggio. While the search warrant application tells us some of the background leading up to the seizure of Mr. Roggio's electronics, many questions remain unanswered, especially those surrounding exactly what occurred at the airport that day. The affidavit references what appears to be a custodial interview of Mr. Roggio at the

airport, but again, more questions than answers regarding that event remain outstanding. A hearing on this motion is necessary to flesh out the facts surrounding the February 26, 2017, seizure of Mr. Roggio's person, his custodial interview, and the seizure and subsequent forensic search of his electronic devices. Whether this was indeed a "border search" can only be determined after a hearing on this motion.

Even If a "Border Search" Occurred, It Was Improper

In *United States v. Whitted, supra,* our Court of Appeals recognized two different classes of border searches, routine and nonroutine. It stated that "routine searches [] require no suspicion and nonroutine searches [] require reasonable suspicion." 541 F.3d at 485. Distinguishing the two, the Court stated "[t]o ascertain whether a border search can be classified as routine, we must examine the degree to which it intrudes on a traveler's privacy… As the Supreme Court has held, 'highly intrusive searches of the person' that implicate the 'dignity and privacy interests of the person being searched' require reasonable suspicion." *Id.* at 485 (*citing United States v. Flores–Montano*, 541 U.S. 149, 152 (2004)). The *Whitted* Court determined that the search of a passenger's cruise ship cabin was nonroutine and, therefore, had to be supported by reasonable suspicion. In making that determination, the Court explained that to "ascertain whether a border search can be classified as routine, we must examine the degree to which it intrudes on a

traveler's privacy." *Id.* It noted that "[c]ourts have focused on the privacy interest and the intrusiveness and indignity of the search to distinguish between routine and nonroutine searches." *Id.* The highly invasive search at issue in this case presents even greater privacy concerns that those presented in *Whitted*, and the forensic search of Mr. Roggio's electronic devices cannot be said to have been routine.

Research has not revealed a Third Circuit case discussing the off-site forensic search of an individual's computer and other electronic devices pursuant to a border search. There are, however, reported cases form other circuits that address this issue.[1] In *United States v. Kolsuz*, 890 F.3d 133, 146 (4th Cir. 2018), the Fourth Circuit held that is was "clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion." The *Kolsuz* case involved a defendant, Hamza Kolsuz, attempting to smuggle arms parts from the United States to Turkey. *Id*. at 136. Kolsuz had a history of attempting to smuggle firearms parts from the United States to Turkey and was caught at the airport attempting to do so in 2012 and 2013. *Id*. at 138. Because of this history, his luggage was searched when he

[1] A divided panel of the Eleventh Circuit, which appears to be on the opposite side of a circuit split than the Third Circuit regarding border searches, held that reasonable suspicion is not required to search *any* property at the border, including electronic devices in *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). In so holding, the Eleventh Circuit cited its prior precedent that held reasonable suspicion was not required to search a crew members cabin. *Id*. at 1233. Because this line of cases is at odds with Third Circuit precedent, *Touset* is inapposite here.

attempted to fly from the Dulles Airport to Turkey in 2016. The search of his luggage revealed 18 handgun barrels, 22 handgun magazines, and a "conversion kit." *Id*. at 139. He was then subjected to a secondary search where his iPhone was taken, sent to a Homeland Security Investigations office, and forensically searched. *Id*. Kolsuz, who was arrested at the airport before his phone was shipped away for analysis, was later charged with various offenses related to the export of firearms. He challenged the search arguing that it should have been considered to be a search incident to arrest rather than a border search. That argument was rejected, and, relevant to the analysis here, the Fourth Circuit addressed the issue of whether reasonable suspicion was necessary to forensically search the iPhone.[2] As noted above, the Court held that it was. In making that determination, the relied heavily on the reasoning in the Supreme Court's decision in Riley *v. California*, ___U.S.___, 134 S.Ct. 2473 (2014), which held that the search incident to arrest exception does not apply to searches of cell phones. The Fourth Circuit recognized the high expectation of privacy in digital devices in current society in determining that the search of such devices – even at the border - could not constitute a routine. It reasoned:

[2] While the *Kolsuz* case is important to this particular analysis, i.e., whether reasonable suspicion is required for a forensic search, as discussed below, this case is distinguishable from *Kolsuz* in many important aspects and a standard even higher the reasonable suspicion should be applied here.

> As described above, the Supreme Court has held that even at the border, individualized suspicion is necessary to justify certain highly intrusive searches, in light of the significance of the individual dignity and privacy interests infringed. Beyond that general guidance, the Court has not delineated precisely what makes a search nonroutine. But as the district court ably explains, in deciding whether a search rises to the level of nonroutine, courts have focused primarily on how deeply it intrudes into a person's privacy….
>
> By that metric, even before the Supreme Court issued its 2014 decision in *Riley*, there was a convincing case for categorizing forensic searches of digital devices as nonroutine….. First is the matter of scale: The sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border—and thus subjected to a routine border search—in luggage or a car. The average 400–gigabyte laptop hard drive can store over 200 million pages. Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage. Subjected to comprehensive forensic analysis, a digital device can reveal an unparalleled breadth of private information.
>
> The uniquely sensitive nature of that information matters, as well. Smartphones and laptops contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails, and also may provide access to data stored remotely…. And finally, while an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind her diaries, photographs, and other especially personal effects, the same is not true, at least practically speaking, when it comes to smartphones and digital devices. Portable electronic devices are ubiquitous—for many, the most reliable means of contact when abroad—and it is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.

Kolsuz, 890 at 144–46. The Court then explained that against a backdrop that already recognized the highly sensitive nature of electronic devices, the Supreme

Court decided *Riley*, which "confirmed every particular of that assessment." *Id*. at 145. According to the Fourth Circuit, "[t]he key to *Rile*y's reasoning is its express refusal to treat such phones as just another form of container, like the wallets, bags, address books, and diaries covered by the search incident exception…. Instead, *Riley* insists, cell phones are fundamentally different 'in both a quantitative and a qualitative sense' from other objects traditionally subject to government searches." *Id*. at 145 (quoting *Riley*, *supra,* 134 S.Ct. at 2489). Thus, the Fourth Circuit in *Kolsuz*, like the Supreme Court in *Riley*, recognized the "immense storage capacity of cell phones, putting a vastly larger array of information at risk of exposure" and the "special sensitivity of the kinds of information" stored on such devices, and the fact that they are a "part of daily life." *Id*. at 145-46. Therefore concluding that border searches of digital devices are nonroutine." *See also United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (requiring a showing of reasonable suspicion to search electronic devices at the border).

Given its reasoning in *United States v. Whitted, supra,* the Third's Circuit's position on border searches is similar to that of the Fourth Circuit in *Kolsuz* and a reasonable suspicion standard, and, at the very least, there must have been reasonable suspicion to justify the forensic search of Mr. Roggio's electronic devices. In *Whitted*, the Court defined the reasonable suspicion standard as follows: "Under the reasonable suspicion standard, customs officers are required

to have a particularized and objective basis to suspect illegal activity in order to conduct a search. … The officers must be able to articulate reasons that led to the search of the cabin that are indicative of behavior in which most innocent people do not engage…. We consider the totality of the circumstances in determining whether reasonable suspicion existed at the time of the search." 541 F.3d at 489. That standard has not been met here. As discussed above – and as will be demonstrated at an evidentiary hearing - the information in the Government's possession at the time that Mr. Roggio arrived at JFK did not rise to the level of reasonable suspicion to justify the forensic search of his electronic devices.

The Probable Cause Standard Should Apply Here

The Third Circuit has not weighed in on this issue yet. At least one dissenting circuit judge has stated that "a forensic search of a cell phone at the border requires a warrant supported by probable cause." *United States v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018) (Pryor, J., dissenting). Judge Pryor's thoughtful dissent relies heavily on the Supreme Court's decision *Riley v. California*, and is more consistent with the Supreme Court's thinking on the searches of electronic devices pursuant to an exception to the warrant requirement. Even the Fourth Circuit in *Kolsuz, supra*, "certain searches conducted under exceptions to the warrant requirement may require more than reasonable suspicion… [and] [p]erhaps the same is true of some nonroutine border searches."

United States v. Kolsuz, 890 F.3d at 148. The defendant in *Kolsuz* was arrested at the airport and taken into custody. He did not "challenge the seizure of his phone, either initially at the airport or later at the Homeland Security Investigations office where it was forensically examined." *Id.* at 141. The Court therefore did not address "whether and under what circumstances an extended confiscation of a traveler's phone—quite apart from any search undertaken—might constitute an unreasonable seizure of property for Fourth Amendment purposes." *Id.* Mr. Roggio, in contrast was not arrested at the airport and was free to leave - without his computers and cell phones, which remained in Government custody. He is certainly challenging the initial confiscation and continued seizure of his electronic devices and his deprivation of the use thereof.

As the facts of this matter are more fully developed at an evidentiary hearing, it will be argued that the circumstances presented herein required a warrant based on probable cause, not one month after his electronics were confiscated and forensically searched, but before. Moreover, it will be demonstrated the even applying the lower reasonable suspicion standard, the seizure and search at issue here cannot stand.

Conclusion

For all of the above reasons, the Defendant, Ross Roggio, respectfully requests that this Honorable Court schedule a suppression hearing.

Respectfully submitted,

Date: March 29, 2019

s/Leo A. Latella

Leo A. Latella
Assistant Federal Public Defender
Attorney ID# PA 68942

201 Lackawanna Avenue, Suite 317
Scranton, PA 18503
(570)343-6285
Fax: (570)343-6225
E-mail: leo_latella@fd.org
Attorney for Ross Roggio

CERTIFICATE OF SERVICE

I, Leo A. Latella, Assistant Federal Public Defender, do hereby certify that this document, the foregoing **Brief in Support of Motion to Suppress**, filed electronically through the ECF system will be sent to the registered Participants as identified on the Notice of Electronic Filing, including the following:

Todd K. Hinkley, Esquire
Assistant United States Attorney

and by placing the same in the United States mail, first class, postage prepaid, at Scranton, Pennsylvania, addressed to the following:

Mr. Ross Roggio

Date: March 29, 2019

s/Leo A. Latella
Leo A. Latella
Assistant Federal Public Defender